Вредоносное программное обеспечение

Вредоносное программное обеспечение - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению, т.е. данные программы способны создавать свои копии. При этом копии программ-вирусов сохраняют способность дальнейшего распространения.

Вредоносное программное обеспечение предполагает несанкционированное использование, т.е. без согласия и ведома пользователя ресурсов персонального устройства и нейтрализацию средств защиты устройства пользователя. Таким образом, вредоносное программное обеспечение, в том числе вирусы, нарушает конфиденциальность, целостность и доступность информации.

Вредоносное программное обеспечение может причинить персональному устройству не меньший вред, чем человеку – вирус серьезной болезни. В названии скрыта главная особенность программы - они схожи с живыми вирусами, распространяясь и живя, но жертвой являются не люди и животные, а компьютеры.

Значительная часть вредоносного программного обеспечения распространяется через сетевые технологии (сетевые, пакетные, почтовые черви и др.) и с помощью средств переноса информации (флэшек, дисков), что позволяет компьютерам «заражать» друг друга вирусами.

Вредоносное программное обеспечение при проникновении на новый носитель информации применяет средства маскировки: он не имеет какого-либо собственного имени: в одних случаях он добавляет свое “тело” программы к уже имеющимся на нем файлам (тем сам заражая их и выступая в дальнейшем под их прикрытием), в других записывает себя, например, как сбойный (дефектный), в третьих размещается в области так называемых старших адресов адресного пространства носителя (винчестера и т.д.), отведенных под оперативную память устройства и т.д. Обычно вредоносное программное обеспечение воздействует на операционную систему, системные и другие важные для работы устройства файлы и память самого устройства.

После проникновения тем или иным способом на носитель информации вирус начинает осуществлять различные действия, которые были ему поставлены ее разработчиком - злоумышленником.

Вредоносное программное обеспечение может повредить, копировать, подменять и полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. Например, вирусы могут украсть пароли, контакты, реквизиты пластиковых карт, а также писать от имени пользователя сообщения в социальных сетях и многое другое.

Яркими примерами работы вредоносного программного обеспечения являются:

1. Троянский конь. Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам).

2. Бэкдор. Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.

3. Технология салями. Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.

В литературе обычно выделяют следующие виды вирусов:

1. Вирус – вредоносный код, который нарушает работоспособность системы, например, отключает интернет, устанавливает экран блокировки, стирает или шифрует файлы, включает возможность удаленного управления твоим компьютером или телефоном.

2. Сетевые черви – это вирусы, которые могут самостоятельно распространяться, заражая все больше устройств.

3. Руткиты – это вирусы, которые маскируют свое присутствие в системе и могут самовосстанавливаться или заражать компьютер при определенных условиях, например, если на компьютере работает администратор.

4. Загрузочные вирусы – это вирусы, поражающие загрузочные сектора дисков.

5. Файловые вирусы – это вирусы, заражающие исполнительные файлы различных типов

6. Шпионские программы – это вредоносные программы, целью которых является слежка и похищение информации. Они могут копировать пароли, контакты, номера пластиковых карт, делать снимки экрана, запоминать нажатия клавиш и другую важную информацию. Позже эта информация передается на сервера злоумышленников. Некоторые вредоносные программы могут отправлять почту, сообщения в социальных сетях, совершать платные звонки и рассылать СМС скрытно от владельца устройства.

Источниками вирусного вредоносного программного обеспечения являются:

1. получение и просмотр вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, которые могут быть получены как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки;

2. открытие файлов на съемных носителях (компакт-диски, флешки и т.д.)

3. посещение зараженных сайтов как специально созданных в целях мошенничества, так и обычных, но имеющих уязвимости информационной безопасности;

4. ошибки программного кода программ, установленных на устройстве;

5. клики по рекламным баннерам сомнительного содержания;

6. скачивание и установка программ из непроверенных или нелицензионных ресурсов.

Зараженный вирусом компьютер часто совершает неожиданные и необычные действия, которые пользователь может заметить, а при их наличии необходимо провести полную проверку системы на наличие вирусов:

1. Снижается скорость обмена данными с Интернетом;

2. Вывод на экран странных сообщений или изображений;

3. Подача странных звуковых сигналов;

4. Неожиданное открытие и закрытие лотка дисковода;

5. Произвольный запуск на компьютере каких-либо программ;

6. Неожиданная перезагрузка и завершение некоторых программ;

7. Повышенная нагрузка и «зависание» устройства;

8. Замедление работы устройства или некоторых программ;

9. Увеличение размера файлов;

10. Появление не существовавших ранее и не создававшихся пользователем файлов;

11. Уменьшение объема доступной оперативной памяти;

12. Искажение содержимого файлов и каталогов или их полное исчезновение;

13. Самопроизвольное появление на экране сообщений или изображений;

14. Странное поведение интернет-браузера;

15. Невозможность перегрузки компьютера (операционная система не загружается).

Вредоносное программное обеспечение как программу сложно обнаружить человеку, а для их выявления и борьбы с ними используются другие программы – антивирусные.

Эти программы в режиме реального времени оценивают все файлы, которые находятся на устройстве, и осуществляют выявление среди них вирусов.

Вирусы постоянно обновляются, совершенствуются, их разработчики нацелены на преодоление антивирусной защиты. Именно по этой причине антивирусные программы имеют базы-энциклопеции вирусов, которые регулярно обновляются, что позволяет производителям антивирусного программного обеспечения оперативно совершенствовать их работу.

Поэтому антивирусные программы нужно не только устанавливать, но и регулярно обновлять.

Обновление происходит следующим образом:

1. Антивирусная программа создает барьер для вирусов, распознавая их. Разработчики антивирусной защиты включают коды известных программ-вирусов в базы данных антивирусных программ.

2. По мере появления новых вирусов антивирусные базы обновляются, и именно эту информацию получает пользователь компьютера, устанавливая обновления антивирусных программ.

Если же вирус проник в компьютер, то существуют антивирусные программы, которые могут «лечить» отдельные зараженные файлы или всю систему. Чаще всего они способны сохранить информацию зараженных файлов полностью или частично.

Также антивирусные программы позволяют перед открытием проверять на наличие вирусов все вставленные в компьютер внешние носители, например, флешки или диски.

Многие производители антивирусных программ предлагают как платные, так и бесплатные решения, которые позволяют обеспечить минимальный уровень безопасности устройств.

Необходимо помнить, что мошенники зачастую предлагают под видом зараженного программного обеспечения бесплатно скачать антивирусную программу, которая распространяется платно ее разработчиком.

Чтобы обезопасить свои устройства от вирусов рекомендуется:

1. Использовать антивирусное программное обеспечение на всех устройствах с регулярным обновлением базы данных (желательно установить автоматическое обновление) и осуществлять регулярную проверку на наличие вирусов. Никогда не отключать антивирус, даже его работа тормозит работу какой-либо программы. Установить максимальные настройки безопасности.

2. Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус. Лучше такое сообщение сразу удалить и очистить корзину.

3. Использовать только лицензионное и актуальное программное обеспечение, в том числе операционную систему и антивирусную программу, и своевременно их обновлять как на компьютере, так и на других устройствах (желательно установить автоматическое обновление или скачивать антивирус только с официального сайта разработчика).

4. Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

5. Не подключать к своему компьютеру непроверенные съемные носители.

6. Включить на компьютере персональный брандмауэр и установить максимальные настройки безопасности.

7. Работать на компьютере под правами пользователя, а не администратора.

8. Ограничить физический доступ к компьютеру для посторонних лиц. Не оставлять без присмотра компьютер с важными сведениями на экране.

9. Регулярно необходимо осуществлять резервное копирование важных данных.

Нужно помнить, что даже антивирусные программы не могут полностью обеспечить и дать стопроцентной гарантии защиты устройства от вирусов, поэтому необходимо внимательно и ответственно использовать сеть «Интернет».

В конце данного раздела отметим, что за создание программ для ЭВМ или внесение в существующие программы изменений, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами предусмотрена уголовная ответственность согласно статье 273 Уголовного кодекса Российской Федерации.

Полномочия по борьбе с распространением вредоносных программ и противодействию мошенническим действиям с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, находятся в сфере деятельности Управления «К» Министерства внутренних дел Российской Федерации.

О создании, распространении и использовании вредоносных программ и других противоправных действиях в сети Интернет можно сообщить в Общественную приемную МВД России на Правоохранительном портале Российской Федерации: www.112.ru